UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
FORT WAYNE DIVISION

LIGTEL COMMUNICATIONS, INC., Plaintiff, v. BAICELLS TECHNOLOGIES INC.; BAICELLS TECHNOLOGIES NORTH AMERICA, INC., Defendants.	Case No. 1:20-cv-00037-HAB-SLC

DECLARATION OF JESSE RAASCH

I, Jesse Raasch, declare the following:

1. I am a citizen of the United States of America, domiciled in the State of Wisconsin.

2. I am employed as Chief Technology Officer and Vice President, Emerging Business, at Baicells Technologies North America Inc. ("Baicells"), a position I have held since April 2015.

3. I have read the Complaint, Declaration of Randy Mead dated January 20, 2020, Declaration of Josh Wentworth dated January 20, 2020, Declaration of Randy Mead filed on April 3, 2020, and Declaration of Josh Wentworth dated April 3, 2020.

4. There is no risk or possibility that an end-user device with a Baicells SIM card using the HNI Code 31198 could be misinterpreted by a network operator as a LigTel device.

5. The process of identifying and authenticating an end-user device to a wireless network is not accomplished by the IMSI alone. That is true regardless of whether the authentication is to the device's home network or to a third-party network. Rather, the process of

identifying an end-user device to a network also requires authentication of the "K" and "OP" or "OPc" values that are programmed on each SIM card.

6. The "K" (sometimes referred to as "Key"), value is the subscriber authentication key, which is unique for each SIM card.

7. The "OP" value is the operator code, which is used for all SIM cards issued by a particular operator. The "OPc" value is the derived operator code and is generated from the OP and K by using an encryption algorithm, which is unique for each SIM card. Since there is no reverse engineering for OPc and it is considered to be more secure than OP, most SIM cards will be coded with OPc instead of OP.

8. The combination of the K and OP/OPc values, along with the IMSI number, are used to authenticate an end-user device to a wireless network.

9. It would be insufficient to rely on an IMSI number alone because those numbers are relatively short and unencrypted, and therefore, they are easily replicable.

10. The required authentication of the K and OP/OPc values, which are secure, encrypted values, is the reason that a Baicells SIM card could not connect to the LigTel network even if the IMSI appeared in plain text to be the same number as that of a LigTel subscriber.

11. The required authentication of the K and OP/OPc values are also the reason that a Baicells SIM card could not connect to a third-party network with which LigTel has a roaming agreement and incur charges as if it were a LigTel customer.

12. The technical process by which roaming occurs is a complex one, but the basic steps demonstrate the impossibility of a Baicells SIM card incurring roaming charges that would be mistakenly attributed to LigTel.

13. First, the end user's device (UE) will perform a cell search procedure and will attempt to attach to the cell belonging to its home network with the strongest signal. If the UE is unable to connect to the home network, and roaming is enabled, the UE will attempt to connect to a cell belonging to another network.

14. Second, when the UE attempts to connect to a cell belonging to another network, it establishes a radio link connection with the eNodeB and through that radio connection it will send an attachment request message. That message contains the IMSI number and will be forwarded to the Mobile Management Entity so that the MME can determine whether there is a roaming agreement in place with the UE's network.

15. Third, if the MME determines that there is a roaming agreement in place, it will contact the central system of that roaming partner's home network and send the IMSI number to request authentication.

16. Fourth, the home network will respond to the MME with authentication vectors for that particular IMSI number, which are generated from the K and OP/OPc values, among other things.

17. Fifth, the MME will then send an authentication request to the UE to ensure that the UE's K and OP/OPc values encoded on its SIM card match exactly those K and OP/OPc values received from the home network.

18. Finally, if those values match exactly, the authentication will be successful. If those values do not match, the authentication will fail.

19. As a result, even assuming that a Baicells SIM card with an IMSI identical to an IMSI assigned by LigTel attempted to connect to a third-party network, the MME would still

deny the connection on authentication because the K and OP/OPc values on a Baicells SIM card would not match those provided by LigTel.

20. For this same reason, there is no risk that any end user of a Baicells network-provider customer could connect to LigTel's network, because neither the K nor OP/OPc values would match those LigTel's system uses to authenticate its users.

21. Thus, there is no risk or possibility that a third-party network provider could mistake an end user of a Baicells network operator for a LigTel customer and enable that end user to incur roaming charges to LigTel.

22. Baicells does not know and does not use LigTel's OP/OPc values, nor does it know or use the K values LigTel assigns to its end user's SIM cards.

23. Baicells does not have any reason to want to know or use LigTel's K or OP/OPc values. Baicells network operators are located all over the United States and provide fixed wireless internet services for their customers. Because the services provided are fixed services, the equipment used by customers is physically mounted on each customer's property and is not mobile. Therefore, customers of the network operators cannot possibly travel out of coverage areas and do not need to roam on other networks.

24. I am aware of instances in which Baicells customers have received requests from law enforcement to obtain the identity of end users suspected of criminal activity. In each such request that I am aware of, law enforcement has identified the Internet Protocol ("IP") address of a suspect and has requested the identity of the end user assigned to that IP address. In my experience, law enforcement officials do not rely on IMSI numbers to identify individuals. Instead, they rely on IP addresses, which do not contain an HNI/PLMN code.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on April 9, 2020 (date) in the State of Wisconsin, United States of America.

Jesse Raasch